**Congruences**

**Theorem:** Let m be a positive integer.
If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then
\( a + c \equiv b + d \pmod{m} \) and \( ac \equiv bd \pmod{m} \).

**Proof:**
We know that \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \)
implies that there are integers s and t with
\( b = a + sm \) and \( d = c + tm \).
Therefore,
\( b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \) and
\( bd = (a + sm)(c + tm) = ac + m(at + cs + stm) \).
Hence, \( a + c \equiv b + d \pmod{m} \) and \( ac \equiv bd \pmod{m} \).

---

**The Euclidean Algorithm**

The **Euclidean Algorithm** finds the **greatest common divisor** of two integers \( a \) and \( b \).
For example, if we want to find \( \gcd(287, 91) \), we **divide** 287 (the larger number) by 91 (the smaller one):
\[
287 = 91 \cdot 3 + 14 \\
\Rightarrow 287 - 91 \cdot 3 = 14 \\
\Rightarrow 287 + 91 \cdot (-3) = 14
\]
We know that for integers \( a, b \) and \( c \),
if \( a \mid b \) then \( a \mid bc \) for all integers \( c \).
Therefore, any divisor of 91 is also a divisor of 91 \( \cdot (-3) \).
Consequently, the greatest common divisor of 287 and 91 must be the same as the greatest common divisor of 14 and 91:
\[
\gcd(287, 91) = \gcd(14, 91).
\]

In the next step, we divide 91 by 14:
\[
91 = 14 \cdot 6 + 7
\]
This means that \( \gcd(14, 91) = \gcd(14, 7) \).
So we divide 14 by 7:
\[
14 = 7 \cdot 2 + 0
\]
We find that 7 \( \mid \) 14, and thus \( \gcd(14, 7) = 7 \).
Therefore, \( \gcd(287, 91) = 7 \).

---

**Representations of Integers**

Let \( b \) be a positive integer greater than 1.
Then if \( n \) is a positive integer, it can be expressed **uniquely** in the form:
\[
n = a_kb^k + a_{k-1}b^{k-1} + \ldots + a_1b + a_0,
\]
where \( k \) is a nonnegative integer,
\( a_0, a_1, \ldots, a_k \) are nonnegative integers less than \( b \),
and \( a_k \neq 0 \).

**Example for \( b=10 \):**
\[
859 = 8 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0
\]
Representations of Integers

Example for \( b=2 \) (binary expansion):
(10110)_2 = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^1 = (22)_{10}

Example for \( b=16 \) (hexadecimal expansion):
(3A0F)_{16} = 3 \cdot 16^3 + 10 \cdot 16^2 + 15 \cdot 16^0 = (14863)_{10}

Representations of Integers

Example:
What is the base 8 expansion of \((12345)_{10}\)?

First, divide 12345 by 8:
12345 = 8 \cdot 1543 + 1
1543 = 8 \cdot 192 + 7
192 = 8 \cdot 24 + 0
24 = 8 \cdot 3 + 0
3 = 8 \cdot 0 + 3

The result is: \((12345)_{10} = (30071)_{8}\).

Representations of Integers

**procedure** base\(_b\)_expansion(n, b: positive integers)
q := n
k := 0
while q \neq 0
begin
   \( a_k := \text{q mod b} \)
   \( q := \lfloor q/b \rfloor \)
   k := k + 1
end
{the base \( b \) expansion of \( n \) is \((a_{k-1} \ldots a_1a_0)_b\)}

Addition of Integers

How do we (humans) add two integers?

Example:
\[
\begin{array}{c}
111 \\
7583 \\
4932 \\
\hline
12515
\end{array}
\]
carry

Binary expansions:
\[
\begin{array}{c}
(1011)_2 \\
+ (1010)_2 \\
\hline
(10101)_2
\end{array}
\]
carry

Addition of Integers

Let \( a = (a_{n-1}a_{n-2} \ldots a_0)_2 \), \( b = (b_{n-1}b_{n-2} \ldots b_0)_2 \).

How can we **algorithmically** add these two binary numbers?

First, add their rightmost bits:
\( a_0 + b_0 = c_0 \cdot 2 + s_0 \),
where \( s_0 \) is the **rightmost bit** in the binary expansion of \( a + b \), and \( c_0 \) is the carry.

Then, add the next pair of bits and the carry:
\( a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1 \),
where \( s_1 \) is the **next bit** in the binary expansion of \( a + b \), and \( c_1 \) is the carry.
Addition of Integers

Continue this process until you obtain \( c_{n-1} \).

The leading bit of the sum is \( s_n = c_{n-1} \).

The result is:

\[
a + b = (s_n s_{n-1} \ldots s_1 s_0)_2
\]

Addition of Integers

Example:

Add \( a = (1110)_2 \) and \( b = (1011)_2 \).

\[
a_0 + b_0 = 0 + 1 = 0 \text{ (2 + 1, so that } c_0 = 0 \text{ and } s_0 = 1).
\]

\[
a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \text{ (2 + 0, so } c_1 = 1 \text{ and } s_1 = 0).
\]

\[
a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \text{ (2 + 0, so } c_2 = 1 \text{ and } s_2 = 0).
\]

\[
a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \text{ (2 + 1, so } c_3 = 1 \text{ and } s_3 = 1).
\]

\[
s_4 = c_3 = 1.
\]

Therefore, \( s = a + b = (11001)_2 \).

Matrices

A matrix is a rectangular array of numbers.

A matrix with \( m \) rows and \( n \) columns is called an \( m \times n \) matrix.

Example:

\[
A = \begin{bmatrix}
-1 & 1 \\
2.5 & -0.3 \\
8 & 0
\end{bmatrix}
\]

is a \( 3 \times 2 \) matrix.

A matrix with the same number of rows and columns is called square.

Two matrices are equal if they have the same number of rows and columns and the corresponding entries in every position are equal.

Matrix Addition

Let \( A = [a_{ij}] \) and \( B = [b_{ij}] \) be \( m \times n \) matrices.

The sum of \( A \) and \( B \), denoted by \( A + B \), is the \( m \times n \) matrix that has \( a_{ij} + b_{ij} \) as its \((i, j)\)th element.

In other words, \( A + B = [a_{ij} + b_{ij}] \).

Example:

\[
\begin{bmatrix}
-2 & 1 \\
4 & 8 \\
-3 & 0
\end{bmatrix} + \begin{bmatrix}
5 & 9 \\
-3 & 6 \\
-4 & 1
\end{bmatrix} = \begin{bmatrix}
3 & 10 \\
1 & 14 \\
-7 & 1
\end{bmatrix}
\]
Matrix Multiplication

Let A be an $m \times k$ matrix and B be a $k \times n$ matrix. The product of A and B, denoted by $AB$, is the $m \times n$ matrix with $(i, j)$th entry equal to the sum of the products of the corresponding elements from the $i$-th row of A and the $j$-th column of B.

In other words, if $AB = \{c_{ij}\}$, then

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \sum_{j=1}^{k} a_{ij}b_{kj}$$

Matrix Multiplication

A more intuitive description of calculating $C = AB$:

- Take the first column of B
- Turn it counterclockwise by 90° and superimpose it on the first row of A
- Multiply corresponding entries in A and B and add the products: $3 \cdot 2 + 0 \cdot 0 + 1 \cdot 3 = 9$
- Enter the result in the upper-left corner of C

- Now superimpose the first column of B on the second, third, …, $m$-th row of A to obtain the entries in the first column of C (same order).

- Then repeat this procedure with the second, third, …, $n$-th column of B, to obtain the remaining columns in C (same order).

- After completing this algorithm, the new matrix C contains the product AB.

Matrix Multiplication

Let us calculate the complete matrix C:

$$A = \begin{bmatrix} 3 & 0 & 1 \\ -2 & -1 & 4 \\ 0 & 0 & 5 \\ -1 & 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 2 & 1 \\ 0 & -1 \\ 3 & 4 \end{bmatrix}$$

$C = \begin{bmatrix} 9 & 7 \\ 8 & 15 \\ 15 & 20 \\ -2 & -2 \end{bmatrix}$